

SECURITY GUARANTEE METHOD FOR PROGRAM DATA INSIDE MEMORY WRITABLE ONLY ONCE

Publication number: JP2000076133

Publication date: 2000-03-14

Inventor: HENDERSON ALVA; FRANCESCO CABARIELE

Applicant: TEXAS INSTRUMENTS INC

Classification:

- international: G06F12/14; G11C16/02; G06F12/14; G11C16/02;
(IPC1-7): G06F12/14; G11C16/02

- european:

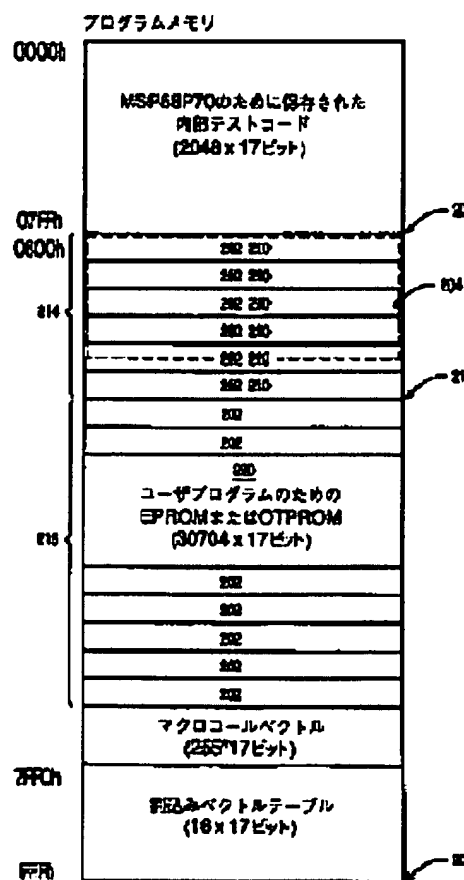
Application number: JP19990158533 19990604

Priority number(s): US19980087957P 19980604; US19980089572P
19980617; US19980090668P 19980625

Report a data error here

Abstract of JP2000076133

PROBLEM TO BE SOLVED: To provide a method for protecting data and a program code stored inside an EPROM array from the act of piracy. **SOLUTION:** After the completion of first programming starting from the first memory address of a nonvolatile memory array 220, a second address 208 from the last functioning as a protective register is set and made to correspond to the number of a protective block 210. For that, a section boundary 212 is set and the array is divided. When the bit 7 (block protection) of the protective register is enabled (set to zero), the contents of a primary security section 214 made non-readable and non-writable. The protective register is written by both of the number of the protective block and the inversion. It prevents the unauthorized change of the protective register and the movement of the section boundary because writing only 0 in the EPROM.



Data supplied from the esp@cenet database - Worldwide

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2000-76133
(P2000-76133A)

(43)公開日 平成12年3月14日(2000.3.14)

(51)IntCl. ⁷	識別記号	F I	テーマコード [*] (参考)
G 0 6 F 12/14	3 1 0	G 0 6 F 12/14	3 1 0 D
G 1 1 C 16/02		G 1 1 C 17/00	6 1 1 Z

審査請求 未請求 請求項の数1 O L (全 9 頁)

(21)出願番号 特願平11-158533

(22)出願日 平成11年6月4日(1999.6.4)

(31)優先権主張番号 0 8 7 9 5 7

(32)優先日 平成10年6月4日(1998.6.4)

(33)優先権主張国 米国 (U S)

(31)優先権主張番号 0 8 9 5 7 2

(32)優先日 平成10年6月17日(1998.6.17)

(33)優先権主張国 米国 (U S)

(31)優先権主張番号 0 9 0 6 6 8

(32)優先日 平成10年6月25日(1998.6.25)

(33)優先権主張国 米国 (U S)

(71)出願人 590000879

テキサス インスツルメンツ インコーポ
レイテッドアメリカ合衆国テキサス州ダラス, ノース
セントラルエクスプレスウェイ 13500

(72)発明者 アルバ ヘンダーソン

アメリカ合衆国 テキサス, シャーマン,
プレストン クラブ ドライブ 228

(72)発明者

フランセスコ カバリエレ
アメリカ合衆国 テキサス, ブラノ, オア
リイ コート 7704

(74)代理人 100066692

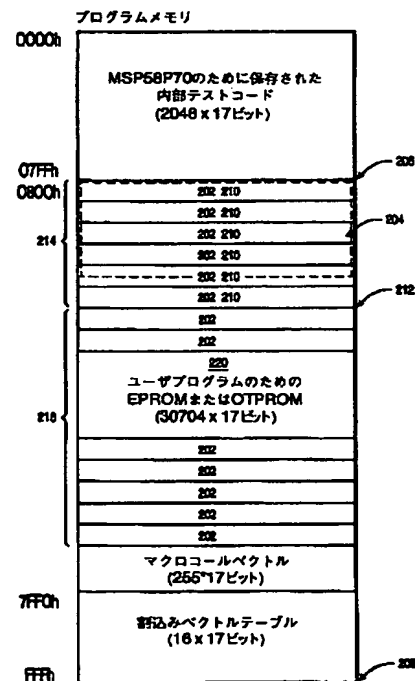
弁理士 浅村 皓 (外3名)

(54)【発明の名称】 一度だけ書き込み可能なメモリ内のプログラムデータのセキュリティ保証方法

(57)【要約】

【課題】 EPROMアレイ内に記憶されたデータとプログラムコードを海賊行為から保護する方法を得る。

【解決手段】 非揮発性メモリアレイ220の第1のメモリアドレスから始まる最初のプログラミングの完了後に、保護レジスタとして働く最後から2番目のアドレス208がセットされて、保護ブロック210の番号と対応する。これは、セクション境界212をセットして、アレイを分割する。1次セキュリティ・セクション214の内容は、保護レジスタのビット7(ブロックプロテクト)がイネーブル(ゼロにセット)されると、読取り不可で書き込み不可にされる。保護レジスタは、保護ブロックの番号およびその反転の両方で書き込まれる。これは、EPROMが0しか書けないことにより、保護レジスタを不正に変更してセクション境界を移動することを防止する。



【特許請求の範囲】

【請求項1】 プログラムメモリと、
複数のプログラムの少なくとも2つのクラスの間の前記プログラムメモリの部分のためのアクセス特権を指示するセキュリティ・レジスタと、
前記プログラムメモリの第1の部分から複数のプログラムの第1のクラスを実行し、前記プログラムメモリの少なくとも1つの他の部分から複数のプログラムの少なくとも1つの他のクラスを実行するために接続されたプログラマブル・プロセッサとを含み、
前記プログラマブル・プロセッサ論理は、前記セキュリティ論理の制御の下においてのみ、また、前記セキュリティ論理がデータ・ポインタとアドレス・ポインタとの間の両立可能な所有権を指示するときのみ、前記メモリにアクセスできる、
集積回路。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、コンピュータ・マイクロプロセッサに関し、特に、1度だけ書込み可能な(OTP)内部メモリを特徴とするマイクロプロセッサに関する。

【0002】

【従来の技術】 コンピュータおよびマイクロコントローラ内のパーマネント・オペレーティング・コード

コンピュータまたはマイクロプロセッサは、典型的には、電源を切っても符号(コード)が保持されるように非揮発性メモリ(たとえば、ROM、EPROM、フラッシュメモリ)内に記憶されたそのオペレーティング・コードの重要部分を有する。しばしば、この符号の全てまたは一部は、中央処理装置(CPU)自体として同一チップ上に常駐するメモリ(内部メモリ)内に記憶される。これにより、CPUおよびその基本オペレーティング・コードを単一ユニットとして実装(パッケージ)可能にしている。単一チップ内での諸機能のこの集積は、プロセッサを使用するアセンブリの設計を単純化するのに役立つ。この集積はまた、部品数(part count)を減少させ、信頼性を向上するのに役立つ。

【0003】 OTPメモリに記憶されたパーマネント・オペレーティング・コード

多くのマイクロプロセッサ、特にマイクロコントローラとして知られるクラスのマイクロプロセッサは、UV消去可能EPROM、EEPROM、1度だけプログラム可能な(OTP)メモリまたはフラッシュメモリのような電氣的にプログラム可能な読取り専用メモリ(EPROM)のある形で、それらの内部オペレーティング・コードを記憶する。この設計により、ICの製造後にオペレーティング・コードをプログラムすることが可能になり、ROMに基づく設計よりも遥かに高度な柔軟性をもたらす。このアーキテクチャーによれば、製造者は、製

造後にオペレーティング・コードを改定し改良したり、オペレーティング・コードを特別の注文により変更して複数の顧客の特別なニーズに応えることができる。代りに、製造者は、EPROMバンクを空白のままにしたり部分的にプログラムして、顧客がその固有のコードをインストールできるようにし得る。この設計により、製造者は一層大量のチップを1度に設定できるようになり、特殊な手持ち在庫の必要を減少させ、迅速なプロトタイプングを容易にする。

【0004】 オンチップ・ソフトウェアのセキュリティ

多くの場合、チップをプログラムする人(製造者または他のパーティ)は、機密保持のために彼が好ましいと思うソフトウェア・コードでチップをプログラムする。そうした場合、先のプログラマーは、後のプログラマーおよびユーザを制約して、チップのメモリバンクからの読取りおよびコピーができないようにするとともに、その中に記憶されたコードの実行のためのアクセスができるようにしておくことを望むであろう。製造者は、チップの内部メモリの一部分をプログラムするとともに、内部メモリの残部を顧客がプログラムするために開放することを望むかもしれない。そうした場合、プログラマーの一方または両方は、他のプログラマーおよび第三者からこのコードを保護しようと望むかもしれない。

【0005】 許可されていないコピーに対するメモリの保護は、複雑で困難な課題である。保護つきメモリは、通常、何かに使用するためにはプロセッサが読めなければならないコードおよびコード関連データを含む。一層問題なことに、CPUの制御を後のプログラマーおよびユーザへ明け渡さなければならず、彼らの多くが先のプログラマーに対して相反する利害を有するであろう。設計においてそれらの道を閉ざすために、あらゆる保護方式は迂回の可能な道を予想しなければならない。

【0006】 現在のメモリセキュリティ方式は、内部メモリバンクを一単位としてロックする。最初のプログラマーがメモリの一部分をプログラムするとともに他の部分を顧客のために残したいと望む場合は、読取りプロテクトを機能抑止のままにして、この最初のプログラマーのソフトウェアが保護されないままにしておかなければならない。装置に精通した人々にとっては、セキュリティ保護を迂回する道が一つ以上あるのが普通であり、これが主としてたまにしか使用しない人に対してそうしたセキュリティを有効なものにしている。

【0007】 アレイの一つだけのプログラマー定義可能セクションの保護が可能であり、このアレイの残りの部分のプログラミングが可能なソフトウェア・セキュリティ方式は、現在のところ存在しない。

【0008】

【発明が解決しようとする課題】 ブロック区分されたセキュリティ・メモリ

本出願は、各パーティのコードについて完全なセキュリ

ティ保護を有する2つ以上のパーティにより装置をプログラムできる方式を記述する。本発明は、製造者が基本ルーチンを装置へプログラムすることを可能にし、また、開発者が各プログラマー・コードについて完全なセキュリティ保護を有する特定アプリケーション用の装置を更にプログラムすることを可能にする。一つの代りの実施の形態において、エンドユーザまたは他の後続のプログラマーが、特定設置に固有な保護つきコードを追加できる。本出願において開示されるセキュリティ回路および制御は、他のプログラマーとともにあらゆる第三者からの海賊行為に対して強力な保護を各プログラマーに提供する。

【0009】

【課題を解決するための手段】好ましい実施の形態では、第1のプログラマーが定義可能な2つ以上のセクションに非揮発性メモリアレイを分割することにより、セキュリティ保護が達成される。一つのセクションがプログラムされロックされると、どのプログラマーもユーザもいずれの保護つきセクションへも読取りまたは書き込みのアクセスができず、確立されたセクション境界も変更できない。命令アドレスと同じメモリセクション内のメモリアドレスをCPUが参照する場合には、読取り命令はCPUによってのみ実行される。異なったセクション内のアドレスを読むことのCPUへの命令は、単純に無視される。

【0010】本出願は、1次セキュリティ方式の迂回を防止するために設計された多数の他の機能を開示する。プロセッサは、コードセクション境界自体の値を保護する機構を採用し、また、保全されたコードを保護するために種々の新規な方式が採用される。CPUは、その内蔵テストモードの一つにある。これらの機構を通じて、競争者や顧客による海賊行為から自分のコードが保全されるという高度の確信をもって、開発者はこのCPU上に彼のコードをインストールできる。

【0011】開示された方法および構造の一つの利点は、メモリの一つのセクションのプログラミングおよび読取りを可能にするとともに、読取りまたはプログラムの操作から安全なセクションを完全に保護することである。

【0012】

【発明の実施の形態】開示される発明は添付図面を参照して説明されるが、これらは本発明の重要な実施の形態を示し、また、本明細書に参考として組み込まれたものを示す。本発明の多数の技術革新的な教示について、現在好ましい実施の形態を特別に参照しながら説明する。しかしながら、このクラスの実施の形態は本明細書の技術革新的な教示の多くの有利な利用のほんの少しの例を提供するだけであることを理解すべきである。一般に、本出願の明細書になされる供述は、必ずしも、本発明の種々のクレームされた発明のいずれかを限定するもので

はない。その上、いくつかの供述は、本発明のいくつかの機能に適用できるが、他の機能には適用できない。

【0013】メモリセクション保護の動作

図2を参照すると、非揮発性メモリ220は、その設計により、2つ以上のブロック202に分割されている。最初のプログラマーによりプログラムされたコード204は、一つ以上のブロック202を占め、第1のメモリアドレス206で始まる。初期プログラミングが完了した後に、アレイ200（保護レジスタ）の最後から2番目のアドレス208が保護ブロック210の数に対応してセットされる。これにより、セクション境界212をセットし、このアレイを1次セキュリティ・セクション214と2次セキュリティ・セクション216とに分割する。1次セキュリティ・セクション214の内容は、保護レジスタ（ブロック保護）のビット7が有効化される（ゼロにセットされる）と、読出し不能で書き込み不能にされる。

【0014】保護値のセキュリティ

好ましい実施の形態では、保護レジスタのビット9～15は、保護されるブロックの番号を反映する値で書き込まれるが、ビット0～6はその値の1の補数（論理反転）で書き込まれる。たとえば、“1011 1001”の1の補数は、“0100 0110”である。この反転値検証方式は、第2のプログラマーの制御の下にあるメモリの部分内に保護レジスタが配置されているという事実により必要とされ、ブロック保護が有効化された後でも変更され得る。本発明で採用されるこの反転値検証方式は、EPROMビットのデフォルト値が1であり、プログラミング中に1ビットをクリアできるが1に戻せない（すなわち、ゼロのみがEPROMセルに書き込まれ得る）という事実の利点を有する。EPROM内の8ビット語は製造者では“1111 1111”を登録する。たとえば、第1のプログラマーは、それを“1111 0000”にプログラムする。それから、この語は、“1010 0000”にプログラムできるが、“1111 0101”にはプログラムできない。

【0015】保護値自体だけがインデックスとして使用される場合には、単に保護コードをクリアするだけで後続のプログラマーがセキュリティ方式を完全に打ち負かすことができる。これにより、セクション境界をゼロにロールバックして、メモリアレイ全体を彼の制御下に置くことができる。その後、このプログラマーは、第1のプログラマーのコードを含むアレイの内容全体をプロセッサの出力ポートの一つにコピーすることができる。

【0016】一方、反転値のみが使用される場合には、保護されてない領域に「トロイの木馬」プログラムを書き込んだのちに保護値をクリアすることによって、後続のプログラマーはこのセキュリティ方式を打ち負かすことができる。これにより、セクション境界をメモリの終点へ移動する。トロイの木馬プログラムは、元のコード

と同じセクション境界の背後にある。その後、セキュリティ回路は、トロイの木馬がメモリアレイ全体にアクセスすることを許容する。その後、このプログラムは、プロセッサの出力ポートにアレイ全体をコピーする。好ましい実施の形態で利用される方式によれば、第2のプログラマーは、ビット0～6を直して、ビット9～15の修正値の補数にすることができない。たとえば、元の保護値が“101 0011”であれば、正しい補数は“010 1100”である。第2のプログラマーはこの保護値を“000 0000”に変えることができる。しかしながら、EPROMに書き込むことができないので、この補数を“0101100”から“1111111”へ変更できない。セキュリティ回路は、この不一致を検出して、アレイへの全ての読取りおよび書込みを機能抑止するであろう。

【0017】メモリ保護回路

いったん保護値がプログラムされ、ブロック保護が使用可能にされると、調べられる命令アドレスおよびアドレスが同一セクション内（すなわち、セクション境界の同一側）にない限り、CPUはどんなテーブル・ルックアップ命令も実行しない。

【0018】このセキュリティチェックを行うために、この装置は、プログラムカウンタ（現に実行される命令のアドレス）およびデータ・ポインタ（現に作用されるメモリアドレス）の両方を保護値と比較する。両方が、保護値よりも高いか低くなければならない。ブロック保護が使用許可になった後で保護値（セクション境界）の同一側にこの2つのアドレスが存在しないと、テーブル・ルックアップまたは書込み命令は何も実行されない。

【0019】このセキュリティチェックを遂行する回路を図1に示す。保護レジスタ184のビット9～15の内容は、プログラムカウンタ・コンパレータ102およびデータポインタ・コンパレータ104の両方の入力Bにロードされる。プロセッサプログラム・カウンタ108の最上位7ビット（すなわち、最寄のブロック全体への命令アドレス）のブロック106が、プログラムカウンタ・コンパレータ106の入力Aにロードされる。プロセッサ・データポインタ112の最上位7ビット（すなわち、最寄のブロック全体への命令オペランドのメモリアドレス）のブロック110が、データポインタ・コンパレータ104の入力Bにロードされる。入力Aの値が入力Bの値よりも大きいか等しければ、各コンパレータ出力が論理「真」を出力する。

【0020】2つのコンパレータ102、104の出力114、116は排他的論理和（XOR）ゲート118に送られる。コンパレータ102、104の出力114、116が異なれば（すなわち、アドレスが異なったセクションにあれば）、XORゲート116の出力120は真であるが、さもなければ、偽である。XORゲート118の出力120は、ANDゲート124の1つの

入力122に送られる。ANDゲート124の他の入力126には、ブロック保護ビット7が供給される。ブロック保護が使用可能にされ、かつ、命令およびオペランド（データ）のアドレスが同一セクション内になれば、ANDゲート124の出力128は真である。この出力128は、以下の仕方で回路により使用される。

【0021】ブロック保護回路の第2の部分は、保護レジスタ内に記憶された保護値で調整することから保護するように設計されている。この回路は、保護値の1の補数（論理反転）であることを期待されるチェック値と保護値を比較する。ブロック保護が使用可能にされるときにチェック値が保護値の反転でなければ、プロセッサは全てのルックアップ命令を完全に機能抑止する。

【0022】この比較を行うための回路も図1に示されている。保護レジスタのビット0～6は、7ビット排他的論理和（XOR）ゲート152の一つの入力150に送られる。保護レジスタのビット9～15は、同じXORゲート152の他の入力154に送られる。ビット0～6の各々がビット9～15の対応するビットの論理反転であれば（すなわち、調整（不正な変更）がなければ）、このゲート152の出力156は偽になる。不一致があれば（すなわち、保護値またはチェック値が不正に変更されていれば）、出力156は真である。XORゲート152の出力156はANDゲート158の一つの側に送られる。ANDゲート158への他の入力160には、保護レジスタ100のブロック保護使用可能ビット7が供給される。反転チェック値に不一致があり、かつ、ブロック保護が使用可能にされていれば、ANDゲート158からの出力162は真である。

【0023】その後、セクタ比較回路からの出力128と保護値セキュリティ回路からの出力162とは、ORゲート164に送られる。このゲート164からの出力166は、他のプロセッサ論理180に送られ、それが真であるときに全てのルックアップ（すなわち、読取り）命令を機能抑止する。したがって、ブロック保護が使用可能にされているときにセクタ境界が突破されるか保護値が不正に変更されれば、プロセッサは全てのルックアップ命令を機能抑止する。更に、この出力166は、第2のORゲート168にも送られる。他の入力170は、保護レジスタからのグローバル保護ビット8の状態を反映する。このORゲート168からの出力172は、他のプロセッサ論理182に送られ、それが真であるときにEPROMアレイへのあらゆる読取りおよび書込み動作を完全に機能抑止する。

【0024】テストモード中のメモリセキュリティ保護
プロセッサのテストモード特にエミュレーションおよびトレース・テストモードの使用を通じて保護メモリへのアクセスをプログラマーが得ることを防止するために、保護の第2の層が装備される。エミュレーション・モードでは、プロセッサは命令を実行しデータレジスタを読

み取るが、これは内部メモリからのように外部メモリからメモリ保護値を読み取ることを含む。トレース・モード（トレース1およびトレース2）では、プロセッサは、ユーザによって制御されたタイミングおよびブレークポイントに従う内部命令を実行する。

【0025】エミュレーション・モードとトレース・モードとの間を自由に移行できることにより、プログラマーがかなり容易にセキュリティ回路を迂回できる。プログラマーは、異なった保護値（たとえば、“00000”）を外部メモリに記憶させて、エミュレーション・モードを使用して新しい保護値の使用をプロセッサに強制できる。その後、彼は、トレース・モードに移行して、内部メモリ内の既に保護されたプログラムを1度に1命令ずつウォーク・スルーすることができる。テスト作業モードがスイッチされる前に装置を初期化するようにプログラマーに強制することにより、このプロセッサは上記策略をブロックできる。初期化に際して、プロセッサは内部EPROMの最期から2番目のメモリ位置から直接に保護値を読み取る。これにより、贋の保護値の使用により引き起こされるセキュリティ回路のあらゆる混乱に対して安全にできる。

【0026】MSP5870プロセッサ・アーキテクチャ
セキュリティ方式は、本来は、消費者電子製品用に設計された低コスト混合信号プロセッサへ組み込まれていた。混合信号プロセッサのブロック図を図3Aおよび図3Bに示す。

【0027】好ましい実施の形態によるプロセッサ10は、プログラムデータメモリブロック11およびデータメモリブロック12を含むいくつかの主要サブブロックを含む。主要サブブロックは、計算ユニット（CU）13と、データメモリアドレスユニット（DMAU）14と、プログラムカウンタ（PCU）15と、命令デコーダ16とを含む。その他の機能は、反復または連鎖カウンタレジスタ17とステータスレジスタ18と2つのタイマ19、20と割り込み論理21と周辺装置拡張インターフェイス22とによって与えられる。

【0028】17ビット・データバス（DB）23が、プロセッサ10内の複数の機能ブロックの間の通信を与える。プロセッサ10内の複数のレジスタの大部分は、DB23への読取りおよび書込みアクセスを有する。不必要な電力消費を避けるために、また、最大の論理伝播時間を与えるために、複数のバス・ドライバ（不図示）はスタティック・デバイスである。プロセッサ10の最小命令周期は約100nsであり、10MHzのプロセッサ・クロック（不図示）が与えられる。

【0029】図3Aのデータメモリ12は、複数の17ビット並列語として編成されている。語の数は、プロセッサ10が適用されるアプリケーションにより異なるが、たとえば256語から2048語の範囲であり、図

3には1152語が示されている。DMAU14により与えられる各アドレス51は、17ビットのデータがアドレスされるようにする。これらの17ビットは、実行される命令により異なる多数の方法で作動することができる。大部分の命令について、このデータは16ビット語フォーマットで解釈される。LACBおよびSACBのような2バイト命令は、バイトフォーマットとも呼ばれる8ビット語フォーマットでプロセッサ10がデータを読み書きするようにさせる。このバイトフォーマット・モードは、アドレスされた16ビット語の上位バイトまたは下位バイトのどちらかをプロセッサのハードウェアが読み書きするようにさせ、取り出されたバイトはDB23で右寄せされる。

【0030】消費者電子製品

このメモリとそれが組み込まれているマイクロプロセッサとは、電話応答機械のような消費者電子製品に使用するように設計されている。本発明を組み込んだ応答機械のブロック図を図4に示す。この装置において、プロセッサ402は、電話線インターフェイス404とマイクロフォン406とスピーカ408とに接続されている。マイクロプロセッサ402は、電話線インターフェイス404経由で電話線410上の音響データを送受信する。マイクロプロセッサはまた、スピーカ408経由で周辺の領域に音響データを送信し、また、マイクロフォン406経由で周辺の領域から音声データを受信できる。

【0031】代りの実施の形態

一つの代りの実施の形態では、この方式は、セキュリティ回路によりブロックされる命令セットが調節される限りにおいて、符号およびデータの両方を保持するメモリアレー（たとえば、フォンノイマン・アーキテクチャ）内に実装できる。このメモリが組み込まれたマイクロプロセッサは、符号およびデータ・バンクは互いに隔離されているハーバード型アーキテクチャに基づいて設計されているが、本発明はこのアーキテクチャに全く限定されない。

【0032】もう一つの代りの実施の形態では、メモリアレーは、二つの保全されたセクションと一つの残りの保全されないままのセクションとに区分される。2つ以上の保全されたセクションが同一データへの読取りアクセスを有することが望ましい場合、または、一つのセクションを開いたままにしておいて、機械にICを設置した後に計算される最終微調整パラメータのセットを記憶させるのが望ましい場合に、これは非常に有用である。

【0033】好ましい実施の形態に関連して使用することが考えられる他の機能や詳細は、クレームされた発明の実施に必ずしも必要でないが、以下の同時係属出願に開示されている。

【0034】代理人ドケット番号T1-24707P、出願番号60/090,670の「可変語長データメモ

り」。

代理人ドケット番号T Iー24708P, 出願番号60/090,589の「チェイン能力つき低コスト乗算器ブロック」。

代理人ドケット番号T Iー24711P, 出願番号60/090,671の「高性能マイクロプロセッサで使用するためのフレキシブル・アキュムレータ・レジスタ・ファイル」。

これら全ては、本出願と共に共通に所有され、本発明の出願日と同実の有効な出願日を有し、本書で援用される。

【0035】修正および変形

当業者に認識されるであろうように、本出願で説明される技術革新的な概念は、非常に広い範囲のアプリケーションにわたり修正され変更し得る。したがって、特許される対称物の範囲は、与えられた特定の例示的な教示のいずれによっても制限されることなく、請求項によってのみ限定される。

【0036】本出願に開示された好ましい実施の形態は、マイクロプロセッサの内部EPROMへ組み込まれていて、2つのセクションに分割されたメモリアレイを記述するが、発明の性質の中には、2つだけのセクションに分割したアレイ、内部メモリ、またはメモリのいずれかの特定のタイプにそのアプリケーションを限定するものは何もない。

【0037】この回路は、このセキュリティ回路を2重化または多重化して追加のセクション領域を収容できる限りにおいて、3つ以上の保全されたセクションを可能にするように修正できる。これは、エンドユーザがメモリ内にパラメータを記憶させる必要がある場合、または、設置後に最終微調整パラメータをメモリに記憶させる必要がある場合に、有用である。

【0038】保全メモリはCPUから独立のIC内におくことができる。他の手段を通じてチップの内容に読取りアクセスするのを防止するために、これは若干の追加のセキュリティまたは暗号回路を必要とするであろう。

【0039】このセキュリティ方式はまた他の形式の非揮発性メモリで実装することもでき、アレイの一部分が読取り専用メモリまたは揮発性メモリでさえあるアレイで実装できる。

【0040】以上の説明に関して更に以下の項を開示する。

(1) プログラムメモリと、複数のプログラムの少なくとも2つのクラスの間の前記プログラムメモリの部分のためのアクセス特権を指示するセキュリティ・レジスタと、前記プログラムメモリの第1の部分から複数のプログラムの第1のクラスを実行し、前記プログラムメモリの少なくとも1つの他の部分から複数のプログラムの少なくとも1つの他のクラスを実行するために接続されたプログラマブル・プロセッサとを含み、前記プログラム

ブル・プロセッサ論理は、前記セキュリティ論理の制御の下においてのみ、また、前記セキュリティ論理がデータ・ポインタとアドレス・ポインタとの間の両立可能な所有権を指示するときのみ、前記メモリにアクセスできる、集積回路。

(2) 前記セキュリティ・アクセス制御論理は、前記セキュリティ・レジスタの前記ビットをチェックして、そのビットの少なくともいくつかは補数の状態にあることを保証し、前記セキュリティ・レジスタは1度だけプログラム可能な非揮発性メモリ技術で実装されている、第1項記載の集積回路。

(3) 前記集積回路はまた、エミュレーション・モードで作動可能であり、他のあらゆるモードで作動する前に前記エミュレーション・モードを去った後に初期化を起らせるハードウェア制約を含む、第1項記載の集積回路。

(4) 前記セキュリティ・レジスタ内の前記補数のフィールドが、前記ブロックの境界を決定する、第1項記載の集積回路。

【0041】(5) メモリアレイであって、複数のセクションにグループされた単一のセル・アレイと、前記アレイ内のセルのいずれかに書き込むために接続された書込み回路と、前記アレイ内のセルのいずれかに書き込むために接続された書込み回路と、前記アレイ内のセルのいずれかから読み出すために接続された読出し回路と、前記読出しおよび書込み回路に接続されたメモリ保護回路であって、セクション境界を決定し、前記セクションの1つに記憶されたいずれかの命令により作動することから前記読出しおよび読書き回路を機能抑止し、また、ひとたびメモリ保護回路が使用許可にされれば前記セクションの他に配置されたいずれかのメモリセルを作動することから前記読出しおよび読書き回路を機能抑止する保護レジスタを組み込んでいるメモリ保護回路と、を含む、メモリアレイ。

【0042】(6) マイクロプロセッサチップであって、再初期化せずにはそのテストモードを変更できない中央処理装置と、該中央処理装置に接続されたプログラムメモリと、プログラムの少なくとも2つのクラスの間で前記プログラムされたメモリの部分へのアクセス特権を指示するセキュリティ・レジスタと、前記メモリに記憶されたデータについて前記メモリの少なくとも第1の部分からプログラムの第1のクラスを実行するとともに第2のクラスを実行するために接続されたプログラマブルプロセッサとを含み、前記セキュリティ論理の制御の下にのみ、また、前記セキュリティ論理がデータ・ポインタとアドレス・ポインタとの間の両立し得る所有権を指示するときのみ、前記プログラマブルプロセッサ論理が前記メモリにアクセスできる、マイクロプロセッサチップ。

【0043】(7) 電話応答機械であって、再初期化せ

ずにはそのテストモードを変更できない中央処理装置と、該中央処理装置に接続されたプログラムメモリと、プログラムの少なくとも2つのクラスの間で前記プログラムされたメモリの部分へのアクセス特権を指示するセキュリティ・レジスタとを含み、前記セキュリティ論理の制御の下にのみ、また、前記セキュリティ論理がデータ・ポインタとアドレス・ポインタとの間の両立し得る所有権を指示する場合にのみ、前記中央処理装置が前記メモリにアクセスでき、メッセージを受信し送信するような方法で前記中央処理装置を電話線に接続するインターフェイスと、前記応答機械内の記憶のために音響を記録するような方法で前記中央処理装置に接続されたマイクロフォンと、前記応答機械内に記憶された音響をプレイバックするような方法で前記中央処理装置に接続されたスピーカとをさらに含む、電話応答機械。

【0044】(8) 本出願は、EPROMアレイ220内に記憶されたデータおよびプログラム・コードを海賊行為から保護する方法を記述する。非揮発性メモリアレイ220は、その設計により2つ以上のブロック202に分割される。最初のプログラマーによりプログラムされたコード204は、1つ以上のブロック202を占め、第1のメモリアドレスから始まる。最初のプログラミングが完了した後に、保護レジスタとして働く最後から2番目のアドレス208がセットされて保護ブロック210の番号と対応する。これは、セクション境界212をセットして、アレイを1次セキュリティ・セクション214と2次セキュリティ・セクション216とに分割する。1次セキュリティ・セクション214の内容

は、保護レジスタのビット7（ブロックプロテクト）が使用可能になる（ゼロにセットされる）と、読取り不可で書き込み不可にされる。保護レジスタは、保護ブロックの番号およびその反転の両方で書き込まれる。これは、EPROMが0しか書けないことにより、保護レジスタを不正に変更してセクション境界を移動することを防止する。

【図面の簡単な説明】

【図1】 開示されるセキュリティ方式を図示する回路図である。

【図2】 セキュリティの理由のために2つのセクションに分割されたメモリアレイを示す図である。

【図3A】 混合信号プロセッサのブロック図である。

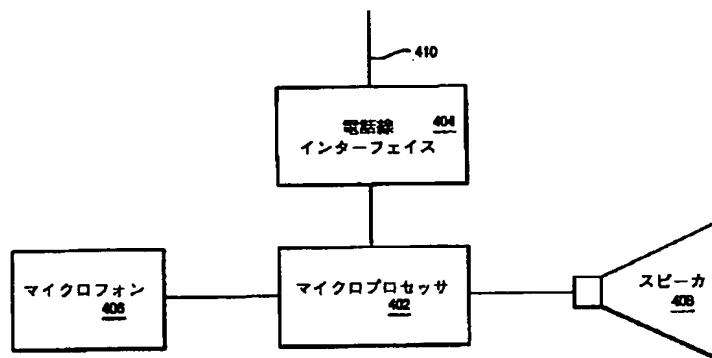
【図3B】 混合信号プロセッサのブロック図である。

【図4】 このメモリアレイを使用する電話応答機械を示す図である。

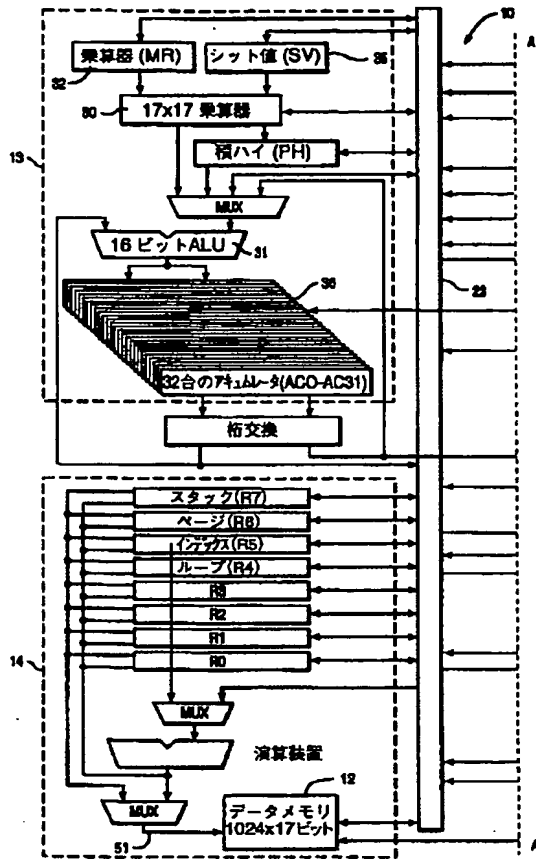
【符号の説明】

- 200 アレイ
- 202 ブロック
- 204 コード
- 206 第1のメモリアドレス
- 208 最後から2番目のアドレス
- 210 保護ブロック
- 212 セクション境界
- 214 1次セキュリティ・セクション
- 216 2次セキュリティ・セクション

【図4】



【図 3 A】



【図 3 B】

